

SECURITY ASSOCIATION CUTTING/CONTINUING METHOD AND COMMUNICATION SYSTEM

Patent Number: JP2003115834
Publication date: 2003-04-18
Inventor(s): TOKINIWA YASUHISA; MIYAGAWA AKIKO; ATOZAWA SHINOBU
Applicant(s): MITSUBISHI ELECTRIC CORP
Requested Patent: ☐ JP2003115834
Application Number: JP20010310596 20011005
Priority Number(s):
IPC Classification: H04L9/08; G06F13/00; G06F15/00; H04L9/32; H04L12/22
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To provide a security association cutting/continuing method, in which arithmetic processing can be reduced.

SOLUTION: In this security association cutting/continuing method, when a user to use a terminal 11 changes the terminal to be used to a terminal 12 during communication using a security association established with a communicating party host 3 by the terminal 11, the terminal 12 updates 'IP address of present terminal' described in the security association related information received from the terminal and according to updated related information, an enciphered security association continuation notice is transmitted to the communicating party host 3. Then, the communicating party host 3 executes prescribed deciphering processing on the received continuation notice and by updating 'IP address of communicating party' described in the security association related information held by that host, the established security association is continued.

Data supplied from the esp@cenet database - I2

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-115834

(P2003-115834A)

(43) 公開日 平成15年4月18日 (2003. 4. 18)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
H 0 4 L 9/08		G 0 6 F 13/00	3 5 3 C 5 B 0 8 5
G 0 6 F 13/00	3 5 3	15/00	3 1 0 E 5 B 0 8 9
15/00	3 1 0	H 0 4 L 12/22	5 J 1 0 4
H 0 4 L 9/32		9/00	6 0 1 D 5 K 0 3 0
12/22			6 7 3 B
審査請求 未請求 請求項の数4 O L (全 15 頁)			

(21) 出願番号 特願2001-310596(P2001-310596)

(22) 出願日 平成13年10月5日 (2001. 10. 5)

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 時庭 康久

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(72) 発明者 宮川 明子

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(74) 代理人 100089118

弁理士 酒井 宏明

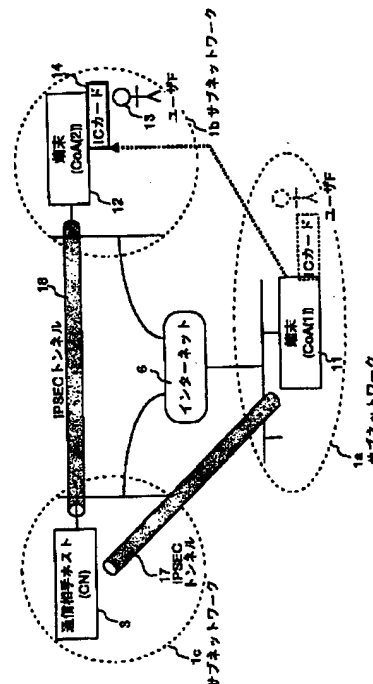
最終頁に続く

(54) 【発明の名称】 セキュリティアソシエーション切断/継続方法および通信システム

(57) 【要約】

【課題】 演算処理を削減可能なセキュリティアソシエーション切断/継続方法を得ること。

【解決手段】 本発明のセキュリティアソシエーション切断/継続方法にあつては、端末11が通信相手ホスト3との間に確立したセキュリティアソシエーションを用いて通信中に、端末11を使用するユーザが使用端末を端末12に変更した場合、端末12が、端末11から受け取ったセキュリティアソシエーション関連情報に記載された「自端末のIPアドレス」を更新し、更新後の関連情報に従って暗号化処理を行ったセキュリティアソシエーション継続通知を通信相手ホスト3に対して送信し、通信相手ホスト3が、受信した継続通知に対して所定の復号処理を行い、自身が保持するセキュリティアソシエーション関連情報に記載された「通信相手のIPアドレス」を更新することによって、上記確立したセキュリティアソシエーションを継続する。



【特許請求の範囲】

【請求項1】 ネットワークを構成する第1の端末が通信相手となる第2の端末との間にセキュリティアソシエーションを確立し、当該セキュリティアソシエーションを用いて暗号通信を行う通信システムのセキュリティアソシエーション切断／継続方法において、

前記第2の端末と通信中に、前記第1の端末を使用するユーザが、当該通信に使用する端末を第3の端末に変更し、その後、前記第3の端末と前記第2の端末との間で通信を行う場合、

前記第3の端末が、前記第1の端末から受け取ったセキュリティアソシエーションに関連する情報に記載された「自端末を識別するための情報」を更新し、更新後のセキュリティアソシエーション関連情報に従って暗号化処理を行ったセキュリティアソシエーション継続通知を生成し、当該継続通知を前記第2の端末に対して送信する継続要求ステップと、

前記第2の端末が、受信した継続通知に対して所定の復号処理を行い、自身が保持するセキュリティアソシエーション関連情報に記載された「通信相手を識別するための情報」を更新することによって、前記確立したセキュリティアソシエーションを継続する継続ステップと、を含むことを特徴とするセキュリティアソシエーション切断／継続方法。

【請求項2】 ネットワークを構成する第1の端末が通信相手となる第2の端末との間にセキュリティアソシエーションを確立し、当該セキュリティアソシエーションを用いて暗号通信を行う通信システムのセキュリティアソシエーション切断／継続方法において、

前記第2の端末と通信中に、前記第1の端末を使用するユーザが、当該通信に使用する端末を第3の端末に変更し、その後、前記第3の端末と前記第2の端末との間で通信を行う場合、

前記第3の端末が、前記第1の端末から受け取ったセキュリティアソシエーションに関連する情報に記載された「自端末を識別するための情報」を更新し、更新後のセキュリティアソシエーション関連情報に従って暗号化処理を行ったセキュリティアソシエーション切断通知を生成し、当該切断通知を前記第2の端末に対して送信する継続要求ステップと、

前記第2の端末が、受信した切断通知に対して所定の復号処理を行い、その後、前記第1の端末と前記第2の端末との間に確立したセキュリティアソシエーションを切断する切断ステップと、

を含むことを特徴とするセキュリティアソシエーション切断／継続方法。

【請求項3】 ネットワークを構成する第1の端末が通信相手となる第2の端末との間にセキュリティアソシエーションを確立し、当該セキュリティアソシエーションを用いて暗号通信を行う通信システムにおいて、

前記第2の端末と通信中に、前記第1の端末を使用するユーザが、当該通信に使用する端末を第3の端末に変更し、その後、前記第3の端末と前記第2の端末との間で通信を行う場合、

前記第3の端末が、前記第1の端末から受け取ったセキュリティアソシエーションに関連する情報に記載された「自端末を識別するための情報」を更新し、更新後のセキュリティアソシエーション関連情報に従って暗号化処理を行ったセキュリティアソシエーション継続通知を生成し、当該継続通知を前記第2の端末に対して送信し、前記第2の端末が、受信した継続通知に対して所定の復号処理を行い、自身が保持するセキュリティアソシエーション関連情報に記載された「通信相手を識別するための情報」を更新することによって、前記確立したセキュリティアソシエーションを継続することを特徴とする通信システム。

【請求項4】 ネットワークを構成する第1の端末が通信相手となる第2の端末との間にセキュリティアソシエーションを確立し、当該セキュリティアソシエーションを用いて暗号通信を行う通信システムにおいて、

前記第2の端末と通信中に、前記第1の端末を使用するユーザが、当該通信に使用する端末を第3の端末に変更し、その後、前記第3の端末と前記第2の端末との間で通信を行う場合、

前記第3の端末が、前記第1の端末から受け取ったセキュリティアソシエーションに関連する情報に記載された「自端末を識別するための情報」を更新し、更新後のセキュリティアソシエーション関連情報に従って暗号化処理を行ったセキュリティアソシエーション切断通知を生成し、当該切断通知を前記第2の端末に対して送信し、前記第2の端末が、受信した切断通知に対して所定の復号処理を行い、その後、前記第1の端末と前記第2の端末との間に確立したセキュリティアソシエーションを切断することを特徴とする通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、通信ネットワークに接続された暗号装置および暗号機能を内蔵した端末が、論理的なセキュリティアソシエーション上で暗号通信を行う場合に用いられるセキュリティアソシエーション切断／継続方法に関するものであり、特に、セキュリティアソシエーション確立時の演算処理を削減可能なセキュリティアソシエーション切断／継続方法および通信システムに関するものである。

【0002】

【従来の技術】以下、従来技術について説明する。RFC 2401～RFC 2412 (RFC: Request For Comments) で規定している IPSEC (IP security プロトコル) では、暗号装置および暗号機能を内蔵した端末が、セキュリティアソシエーションと呼ばれ

る論理的な通信路上で暗号通信を行う。セキュリティアソシエーションでは、暗号通信を行う二者間で通信を開始する前に、暗号用鍵と認証用鍵とを共有する。暗号用鍵と認証用鍵とを共有し、セキュリティアソシエーションを確立する手順が、IKE (Internet Key Exchange) の通信手順である。IKEは、RFC 2408およびRFC 2409で規定されている。

【0003】図9は、たとえば、特開2000-332825号公報に示された従来のセキュリティアソシエーション切断/継続方法を示す図である。図9において、101a、101b、101cはサブネットワークであり、106はサブネットワーク101a、101b、101cを相互接続しているインターネットであり、102はサブネットワーク101aに存在する移動端末であり、103は通信相手ホストであり、104は移動端末102の現在位置アドレスおよび移動の有無を管理するためのDNS (Domain Name System) サーバであり、107はセキュリティアソシエーションとして確立したIPSECトンネルである。

【0004】つぎに、上記システムの動作について説明する。ここでは、移動端末102が、サブネットワーク101aから他のサブネットワーク101bに移動した状態で、ネットワーク101cにある通信相手ホスト（固定ノード：CN）103と通信する場合について説明する。また、移動中の移動端末102と通信相手ホスト103との間の通信には、IPSECのトンネルモード (Tunnel Mode) を使用する (IPSECの詳細についてはRFC 2401～RFC 2412参照)。

【0005】移動端末102は、一意に識別可能な一つのアドレスを持つ。これをホームアドレス (Home Address: Haddr) と呼ぶ。ホームアドレスは、移動端末102が所属するサブネットワーク101aにおいて割り当てられる。また、移動端末102は、訪問先のネットワークで適切なアドレスを少なくとも一つ獲得する。これをケア・オブ・アドレス (Care-of Address: CoA) と呼ぶ。

【0006】また、移動端末102では、トンネルモードIPSEC通信の際、付与されたIPアドレス (CoA) を、IPSECトンネルの一端 (終端点) を示すアドレス (ゲートウェイアドレス) として使用する。Haddrは、カプセル化された内部パケットにおける送信元アドレスとして使用される。

【0007】また、移動端末102では、移動した場合に、自装置内で使用されるCoAを更新する。このとき、移動端末102では、DNSサーバ104に新たに獲得したCoAを通知する。

【0008】一方、通信相手ホスト103では、上記CoAの更新処理の代わりに、移動端末102から受信した情報に基づいて自装置内で使用する移動端末102のCoAを更新する。

【0009】また、通信相手ホスト103では、移動端末102に発呼する際に、移動端末102のCoAをDNSサーバ104に問い合わせる。また、通信相手ホスト103では、トンネルモードIPSEC通信における外側パケットおよび内側パケットの2種類のアドレスに、同じアドレス (CN) を使用する。

【0010】図10は、移動端末102から通信相手ホスト103へIPSECトンネル107を用いてパケットを転送する様子を示す図である。図10において、108はIPSECトンネルである。

【0011】移動端末102では、サブネットワーク101aで現在位置を示すCoAとしてCoA (1) を獲得する (RFC 2002で規定されるCo-located Care-of addressで動作する)。ここでは、獲得したCoA (1) を、IPパケット自体のオリジナルの送信元アドレスとするのではなく、IPSECトンネルの一端を示すアドレス (ゲートウェイアドレス) とし、ホームアドレス (Haddr) を、IPパケット自体のオリジナルの送信元アドレスとして、通信を行う。すなわち、図10に示すように、カプセル化した外側パケットの送信元アドレス (src) を“CoA (1)” とし、宛先アドレス (dst) を“CN” とし、内側パケットのオリジナルの送信元アドレス (src) を“Haddr” とし、最終的な宛先アドレス (dst) を“CN” とするカプセル化パケットが転送される。

【0012】つぎに、移動端末102が移動し、現在位置を示すCoAが“CoA (1)” から“CoA (2)” に変化した場合のアドレスの切り替えについて説明する。

【0013】この場合、移動端末102では、CoAが“CoA (2)” に変わった時点で、IPSECトンネルの外側パケットの送信元アドレスを“CoA (2)” に変更する。その結果、図10に示すように、外側パケットの送信元アドレスが“CoA (2)” に変更されたカプセル化パケットが転送される。

【0014】移動端末102のCoAの変化を検出した通信相手ホスト103では、IPSECのセキュリティアソシエーション (セキュリティの関連情報) のデータベース: SADを参照し、このセッションの宛先ゲートウェイアドレスを“CoA (1)” から、新たに“CoA (2)” に置き換える。このとき、通信相手ホスト103では、ゲートウェイアドレス以外のセキュリティアソシエーション情報を変えないので、たとえば、IPSECの暗号化、認証鍵などを再度折衝する必要がない。

【0015】また、移動端末102では、CoAが切り替わった時点で、DNSサーバ104に対して更新メッセージを送信する。DNSサーバ104では、通常のフィールド (ドメイン名、アドレスレコード (IPv6ではAAAA) 等) に加え、移動端末のホームアドレス

(Haddr)のための拡張フィールド(Home Address Resource Record: HAAAA)を持つ。また、アドレスレコード(IPv6ではAAAA)には、Haddr(移動していないとき)またはCoA(移動しているとき)が記述される。

【0016】移動端末102は移動先で新規のCoAを取得すると、アドレスレコードを動的に更新するため、通信相手ホスト103では、アドレスレコードと拡張フィールド:HAAAAとが異なる場合に、移動端末102が移動先でCoAを取得して接続していることを知ることができる。

【0017】なお、DNSサーバ104に対するHAAAAの問い合わせや、HAAAAフィールドやアドレスレコードの動的更新は、従来から行われていたIPアドレスの問い合わせ方式や動的DNS更新処理(例:RFC2136)を拡張して容易に定義できる。

【0018】また、DNSサーバ104上のHAAAA情報は、たとえば、通信相手ホスト103が移動端末102に対してパケットを送信し、移動端末102がこれを着呼できるような場合に使用する。すなわち、通信相手ホスト103では、DNSサーバ4に対して問い合わせを行い、CoAが登録されている移動端末102に対してパケットを送信する場合、IPSECのトンネルモードを使用してトンネルの宛先アドレス(ゲートウェイアドレス)をCoAにしてセキュリティアソシエーションを構成し、さらに、セキュリティアソシエーションのデータベースを保持し、正しい現在位置にパケットを送信する。

【0019】つぎに、IPSECにおける処理の概要について説明する(IPSECの詳細についてはRFC2401~RFC2412参照)。

【0020】IPSECの処理は、セキュリティアソシエーション(Security Association)に記述された内容に従って行われる。セキュリティアソシエーションは、セキュリティ・パラメータ・インデックス(Security Parameter Index: SPI)とdst(宛先アドレス)の組から一意に定まる、IPSECに関する情報の集合である。SPIは、セキュリティアソシエーションを定めるために使用される32bitの整数のインデックスであり、AH(Authentication Header)、ESP(Encapsulating Security Payload)のヘッダ内に記述され、セキュリティアソシエーションの選択に使用される。セキュリティアソシエーションに記述される主な内容は、dst, SPI, プロトコル(ESP(もしくはAH)、モード(tunnel))、AHまたはESPで使用されるアルゴリズムと鍵などである。

【0021】IPSECを使用するためには、使用前に、通信相手とセキュリティアソシエーションの内容について合意するための手続を行う。セキュリティアソシエーションの管理は、鍵管理プロトコル: IKEの果た

すべき役割である。鍵管理プロトコル: IKEでは、「DiffieHellman」と呼ばれる数学的なべき乗剰余演算によって共有鍵を共有する。また、相互認証には、X.509の認証書を用いたRSA(Ron Rivest, Adi Shamir, Leonard Adleman)演算によりべき乗剰余演算を行うモードも規定されている。

【0022】パケットを送信する場合は、まず、セキュリティ・ポリシー・データベース: SPD(Security Policy Database)を検索する。SPDは、対象となるパケットのsrc/dst等の要素から、セキュリティ・ポリシーを選択する。セキュリティ・ポリシーは、「パケットを破棄する(discard)」、「パケットをそのまま通過させる(bypass)」、「IPSECの処理を行う(apply)」の行動を定めるものである。たとえば、セキュリティ・ポリシーが「apply」の場合には、使用するセキュリティアソシエーション(あるいはセキュリティアソシエーションが満たすべき条件)が記述されている。そして、使用するセキュリティアソシエーションが定まるので、これに記述された内容に従って対象のパケットに対して暗号などの処理を行う。なお、セキュリティアソシエーションがない場合は、適切な鍵共有プロトコル: IKEを使用してセキュリティアソシエーションの確立を行う。

【0023】一方、IPSECが使用されているパケットを受信すると、まず、受信した端末は、dst(通常は受信したノード)とSPIから、セキュリティアソシエーションを決定し、記述された内容に従ってIPSECの復号などの処理を行う。この結果、得られたパケットをもとにSPDを検索し、セキュリティ・ポリシーを得る。そして、セキュリティ・ポリシーから導かれるセキュリティアソシエーションが、このパケットを処理するために使用してきたセキュリティアソシエーションと一致するかどうかを確認する。

【0024】図11は、移動端末102および通信相手ホスト103が接続されたネットワークの動作手順を示す図である。ここでは、サブネットワーク101aに存在する移動端末102(CoA=CoA(1))が通信相手ホスト103と通信を行う場合について説明する。図12は、この場合の動作シーケンスの一例を示す図である。

【0025】まず、移動端末102では、適切な鍵管理プロトコル: IKEを使用して通信相手ホスト103とのセキュリティアソシエーション: SAを確立する(ステップS101)。

【0026】図13は、移動端末102および通信相手ホスト103が持つセキュリティ・ポリシー・データベース: SPDの一例を示す図である。また、図14は、移動端末102および通信相手ホスト103が持つセキュリティアソシエーション・データベース: SADの一例を示す図である。なお、使用するIPSECプロトコ

ルはESPを想定する。

【0027】移動端末102が通信相手ホスト103に対してパケットを送信する場合、移動端末102では、図13(a)のSPDを検索し、識別名：SPM(1)を選択する。SPM(1)にはセキュリティアソシエーション：SAとしてSAM(1)を参照するように記述されているので、図14(a)のSAM(1)を参照する。SAM(1)には、Destinationアドレスとして“CN”が、protocolとして“ESP”が、modeとして“tunnel”が指定されているので、移動端末102から通信相手ホスト103へのパケットをIPSECでカプセル化し、そのパケットのDestinationアドレスを“CN”、SPIを“c(1)”として送信する(ステップS102)。

【0028】このパケットを受け取った通信相手ホスト103では、(dst, SPI) = (CN, c(1))であるセキュリティアソシエーションを、図14(b)に示すSADから検索する。その結果、得られたセキュリティアソシエーションを使用してESPを検証し、カプセル化を外して通信相手ホスト103へのパケットを生成する。通信相手ホスト103から移動端末102へのパケットも上記と同様に送信される(ステップS103)。

【0029】移動端末102および通信相手ホスト103のアプリケーションは、通信がすべて“Haddr”と“CN”との間で行われていると認識するが、実際にネットワークを流れるパケットは、“CoA(1)”と“CN”との間のパケットとなる。

【0030】この状態で、移動端末102がサブネットワーク101bに移動して“CoA(2)”を取得した場合、移動端末102では、次の3つの処理を行う。

①Dynamic DNS Update

移動端末102に対応するAAAAフィールドに、現在のCoAである“CoA(2)”を登録する(ステップS104)。

②SA Gateway Update

dstフィールドが“CoA(1)”でないセキュリティアソシエーションを検索すると、dst=CNがあるので、“CN”に対して「SA Gateway Update」を行う(ステップS105)。その結果、図14(b)のセキュリティアソシエーション・データベース：SADの内容は、図14(d)のように更新される。

③SA Local Update

移動端末102では、自身のSADを検索し、dstフィールドが“CoA(1)”であるものについて、すべて“CoA(2)”へと変更する。

【0031】移動端末102が現在通信している相手は、すべてのセキュリティアソシエーションのdestinationアドレスが現在のCoAである“CoA

(2)”に変化するため、IPSECトンネルのend pointは、“CoA(1)”から“CoA(2)”に切り替わる。これにより、移動端末102が移動した場合でもセッションが保証される(ステップS106、S107)。その結果、図14(a)のセキュリティアソシエーション・データベース：SADの内容は、図14(c)のように更新される。

【0032】このように、従来技術では、標準のプロトコルであるIPSECのトンネルモードを利用して、通信相手との通信路を確保する。さらに、「SA Gateway Update」という概念を追加することで、トンネルの終端点の変更を可能にし、移動後のセッションを保証する。また、「Dynamic DNS Update」を利用するとともに、新たに「Home Address Resource Record(HAAAA)」をDNSに導入する。これにより、移動端末のホームアドレスとCoAとの関係を知ることができ、その結果、ホームアドレスを移動端末の識別子として使用できる。

【0033】

【発明が解決しようとする課題】しかしながら、上記、従来のセキュリティアソシエーション切断/継続方法においては、端末自体が移動することについては考慮しているが、ユーザが使用する端末を変更した場合には全く対応していない。すなわち、ユーザがICカードにX.509の認証書を保持し端末間を移動した場合は、ユーザが移動した端末においてもセキュリティアソシエーションを再確立し、そのとき、鍵共有プロトコル：IKEでは「DiffieHellman演算」や「RSA演算」のべき乗剰余演算が発生するため、多大な演算時間が必要となり、さらに、リソースも消費してしまう、という問題があった。

【0034】特に、クライアントサーバモデルにおけるサーバ側において、何万〜何百万のクライアントユーザの鍵共有処理を実施する場合には、これらのべき乗剰余演算を減らす必要がある。

【0035】また、上記、従来のセキュリティアソシエーション切断/継続方法においては、不必要になったセキュリティアソシエーションを寿命が終了するまで維持し続けることになるため、無駄なリソースを消費する、という問題もあった。

【0036】本発明は、上記に鑑みてなされたものであって、ユーザが移動し通信に使用する端末を変更した場合の、べき乗剰余演算処理を削減することが可能なセキュリティアソシエーション切断/継続方法および通信システムを得ることを目的とする。また、端末移動後の不必要なセキュリティアソシエーションを切断することが可能なセキュリティアソシエーション切断/継続方法および通信システムを得ることを目的とする。

【0037】

【課題を解決するための手段】上述した課題を解決し、目的を達成するために、本発明にかかるセキュリティアソシエーション切断／継続方法にあつては、ネットワークを構成する第1の端末（後述する実施の形態の端末11に相当）が通信相手となる第2の端末（通信相手ホスト3または中継装置に相当）との間にセキュリティアソシエーションを確立し、当該セキュリティアソシエーションを用いて暗号通信を行う通信システムにおいて、前記第2の端末と通信中に、前記第1の端末を使用するユーザが、当該通信に使用する端末を第3の端末（端末12に相当）に変更し、その後、前記第3の端末と前記第2の端末との間で通信を行う場合、前記第3の端末が、前記第1の端末から受け取ったセキュリティアソシエーションに関連する情報に記載された「自端末を識別するための情報」を更新し、更新後のセキュリティアソシエーション関連情報に従って暗号化処理を行ったセキュリティアソシエーション継続通知を生成し、当該継続通知を前記第2の端末に対して送信する継続要求ステップと、前記第2の端末が、受信した継続通知に対して所定の復号処理を行い、自身が保持するセキュリティアソシエーション関連情報に記載された「通信相手を識別するための情報」を更新することによって、前記確立したセキュリティアソシエーションを継続する継続ステップと、を含むことを特徴とする。

【0038】つぎの発明にかかるセキュリティアソシエーション切断／継続方法にあつては、ネットワークを構成する第1の端末が通信相手となる第2の端末との間にセキュリティアソシエーションを確立し、当該セキュリティアソシエーションを用いて暗号通信を行う通信システムにおいて、前記第2の端末と通信中に、前記第1の端末を使用するユーザが、当該通信に使用する端末を第3の端末に変更し、その後、前記第3の端末と前記第2の端末との間で通信を行う場合、前記第3の端末が、前記第1の端末から受け取ったセキュリティアソシエーションに関連する情報に記載された「自端末を識別するための情報」を更新し、更新後のセキュリティアソシエーション関連情報に従って暗号化処理を行ったセキュリティアソシエーション切断通知を生成し、当該切断通知を前記第2の端末に対して送信する継続要求ステップと、前記第2の端末が、受信した切断通知に対して所定の復号処理を行い、その後、前記第1の端末と前記第2の端末との間に確立したセキュリティアソシエーションを切断する切断ステップと、を含むことを特徴とする。

【0039】つぎの発明にかかる通信システムにあつては、ネットワークを構成する第1の端末が通信相手となる第2の端末との間にセキュリティアソシエーションを確立し、当該セキュリティアソシエーションを用いて暗号通信を行う構成とし、たとえば、前記第2の端末と通信中に、前記第1の端末を使用するユーザが、当該通信に使用する端末を第3の端末に変更し、その後、前記第

3の端末と前記第2の端末との間で通信を行う場合、前記第3の端末が、前記第1の端末から受け取ったセキュリティアソシエーションに関連する情報に記載された「自端末を識別するための情報」を更新し、更新後のセキュリティアソシエーション関連情報に従って暗号化処理を行ったセキュリティアソシエーション継続通知を生成し、当該継続通知を前記第2の端末に対して送信し、前記第2の端末が、受信した継続通知に対して所定の復号処理を行い、自身が保持するセキュリティアソシエーション関連情報に記載された「通信相手を識別するための情報」を更新することによって、前記確立したセキュリティアソシエーションを継続することを特徴とする。

【0040】つぎの発明にかかる通信システムにあつては、ネットワークを構成する第1の端末が通信相手となる第2の端末との間にセキュリティアソシエーションを確立し、当該セキュリティアソシエーションを用いて暗号通信を行う構成とし、たとえば、前記第2の端末と通信中に、前記第1の端末を使用するユーザが、当該通信に使用する端末を第3の端末に変更し、その後、前記第3の端末と前記第2の端末との間で通信を行う場合、前記第3の端末が、前記第1の端末から受け取ったセキュリティアソシエーションに関連する情報に記載された「自端末を識別するための情報」を更新し、更新後のセキュリティアソシエーション関連情報に従って暗号化処理を行ったセキュリティアソシエーション切断通知を生成し、当該切断通知を前記第2の端末に対して送信し、前記第2の端末が、受信した切断通知に対して所定の復号処理を行い、その後、前記第1の端末と前記第2の端末との間に確立したセキュリティアソシエーションを切断することを特徴とする。

【0041】

【発明の実施の形態】以下に、本発明にかかるセキュリティアソシエーション切断／継続方法および通信システムの実施の形態を図面に基づいて詳細に説明する。なお、この実施の形態によりこの発明が限定されるものではない。

【0042】実施の形態1．図1は、本発明にかかるセキュリティアソシエーション切断／継続方法を実現する通信システムの構成を示す図である。図1において、1a、1b、1cはサブネットワークであり、6はサブネットワーク1a、1b、1cを相互接続するインターネットであり、3は通信相手ホスト（CN）であり、11はサブネットワーク1aに存在する端末であり、12はサブネットワーク1bに存在する端末であり、13はユーザFであり、14はユーザFの認証書とSPD（Security Policy Database）とSAD（Security-Association Database）情報を格納するICカードであり、17は通信相手ホスト3と端末11間でセキュリティアソシエーションとして確立されたIPSECトンネルであり、18は通信相手ホスト3と端末12間でセキュリテ

ィアソシエーションとして確立されたIPSECトンネルである。

【0043】ここで、上記ネットワークにおける実施の形態1のセキュリティアソシエーション切断/継続方法について説明する。ここでは、ユーザFが、サブネットワーク1aに属する端末11を用いて通信相手ホスト3と通信を行い、その後、移動先のサブネットワーク1bに属する端末12を用いて通信相手ホスト3と通信を行う場合について説明する。

【0044】なお、移動前の端末11と通信相手ホスト3との間の通信、および移動後の端末12と通信相手ホスト3との間の通信には、IPSECのトンネルモード(Tunnel Mode)を使用する(IPSECの詳細についてはRFC2401～RFC2412参照)。また、端末11は、CoA(1)の固定IPアドレスを持ち、端末12は、CoA(2)の固定IPアドレスを持ち、通信相手ホスト3は、CNの固定IPアドレスを持つ。また、端末11と端末12と通信相手ホスト3は、トンネルモードIPSEC通信における外側パケットおよび内側パケットの2種類のアドレスには、同じIPアドレスを使用する。

【0045】図2は、IPSECを用いた端末間の通信の様子を示す図である。パケットを送信する場合、各端末では、セキュリティ・ポリシー・データベース：SPDを検索する。SPDは、対象となるパケットのsrc(sourceアドレス)およびdst(Destinationアドレス)等の要素から、セキュリティ・ポリシーを選択する。セキュリティ・ポリシーは、「パケットを破棄する(discard)」、「パケットをそのまま通過させる(bypass)」、「IPSECの処理を行う(apply)」の行動を定めるものである。たとえば、セキュリティ・ポリシーが「apply」の場合には、使用するセキュリティアソシエーション(あるいはセキュリティアソシエーションが満たすべき条件)が記述されている。この場合、使用するセキュリティアソシエーションが定まるので、これに記述された内容に従って対象のパケットに対して暗号などの処理を行う。

【0046】一方、セキュリティアソシエーションがない場合は、適切な鍵共有プロトコル：IKEを使用してセキュリティアソシエーションの確立を行う。鍵共有プロトコル：IKEでは、なりすまし防止のために相互認証を行っている。なお、パスワードのような秘密情報を二者間で共有した事前共有鍵による認証方式以外に、X.509の認証書を用いたデジタル署名により相互認証を行う方式、を規定している。デジタル署名では、装置毎あるいはユーザ毎に認証局が発行した認証書を用いる。

【0047】IPSECが使用されているパケットを受信した端末では、dst(通常は受信したノード)とS

PI(Security Parameter Index)から、セキュリティアソシエーションを決定し、記述された内容に従ってIPSECの復号などの処理を行う。そして、得られたパケットをもとにSPDを検索し、セキュリティ・ポリシーを得る。その後、セキュリティ・ポリシーから導かれるセキュリティアソシエーションが、このパケットを処理するために使用してきたセキュリティアソシエーションと一致するかどうかを確認する。

【0048】図3は、ユーザFが端末11から端末12へ移動した場合の動作シーケンスの一例を示す図である。なお、使用するIPSECプロトコルはESP(Encapsulating Security Payload)を想定する。まず、端末11では、適切な鍵管理プロトコル：IKEを使用して通信相手ホスト3とのセキュリティアソシエーション：SAを確立する(図3、ステップS1、(1)参照)。セキュリティアソシエーション：SAを確立するための識別子は、端末11がユーザFのID(詳細にはX.509のユーザFの認証書のsubject名)であり、通信相手ホスト3が自局のIPアドレス：CNまたは通信相手ホスト3の認証書のIDである。

【0049】端末11では、通信相手ホスト3に対してTCP(Transmission Control Protocol)/UDP(User Datagram Protocol)のport番号80のパケットを送信する場合、SPDを検索する。図4は、ユーザFのICカード内のSPD、ユーザGのICカード内のSPD、通信相手ホスト3内のSPD、を示す図であり、特に、図4(a)は、セキュリティアソシエーション：SAを確立する前にICカード14内に設定されているユーザFのセキュリティ・ポリシー・データベース：SPDの一例を示す図である。図4(a)の検索処理により、ここでは、SPF(1)を選択する。

【0050】SPF(1)にはセキュリティアソシエーションとしてSAF(1)を参照するように記述されているので、端末11では、図5(a)のSAF(1)を参照する。図5は、ユーザFに関するSADを示す図であり、特に、図5(a)は、セキュリティアソシエーション：SAを確立した後に生成される端末11のセキュリティアソシエーション・データベース：SADの一例を示す図である。

【0051】SAF(1)には、Destinationアドレスとして“CN”が、protocolとして“ESP”が、modeとして“tunnel”が、それぞれ指定されているので、端末11では、通信相手ホスト3へのパケットをIPSECでカプセル化し、そのパケットのsourceアドレスを“CoA(1)”とし、Destinationアドレスを“CN”とし、SPIを“h(2)”とし、ESPにこれらを付与して送信する(図3、ステップS2、(2)参照)。カプセル化の処理では、暗号鍵：KEYH(2)を用いて内側のパケットを暗号化する。

【0052】このパケットを受信した通信相手ホスト3では、(dst, SPI) = (CN, h(2))であるセキュリティアソシエーションを、図6(a)に示すSADから検索する。図6は、通信相手ホスト3に関するSADを示す図であり、特に、図6(a)は、セキュリティアソシエーション：SAを確立した後に生成される通信相手ホスト3のセキュリティアソシエーション・データベース：SADの一例を示す図である。検索の結果、通信相手ホスト3では、得られたセキュリティアソシエーションを使用してESPを検証し、カプセル化を外して端末11からのパケットを得る。カプセル化を外す処理では、暗号鍵：KEYH(2)を用いて内側のパケットを復号する。

【0053】そして、通信相手ホスト3および端末11では、通信相手ホスト3から端末11へのパケットについても上記と同様の手順で処理する(図3、ステップS3、(3)参照)。

【0054】つぎに、図1において、ユーザFが端末11から端末12へ移動し、端末12と通信相手ホスト3との間で通信を行う場合について説明する。まず、ユーザFは、図5(a)に示されているSADをICカード14へコピーし、移動後に、ICカード14の内容を端末12へ書き込む。端末12では、図5(a)の受信用SAF(2)のDestinationアドレスが端末12の自局アドレスと異なるため、CoA(1)を端末12のIPアドレスであるCoA(2)へ変更する。その結果、図5(a)のセキュリティアソシエーション・データベース：SADの内容は、図5(b)のように更新される。

【0055】さらに、端末12では、ユーザFに関するセキュリティアソシエーション・データベース：SADに従ってセキュリティアソシエーション：SAの継続を通信相手ホスト3へ通知する(図3、ステップS4、(4)参照)。ここでは、Sourceアドレスを“CoA(2)”とし、destinationアドレスを“CN”とし、SPIを“h(2)”とし、ESPにこれらを付与する。そして、内側のパケットのsourceアドレスを“CoA(2)”とし、destinationアドレスを“CN”とし、port番号を“10000”とし、データ部にSAを継続するコードとユーザFの認証書のsubject名を設定し、暗号鍵：KEYH(2)を用いて暗号化後、IPSECでカプセル化する。

【0056】SAの継続通知を受信した通信相手ホスト3では、(dst, SPI) = (CN, h(2))であるセキュリティアソシエーションを、図6(a)のSADから検索する。ここでは、SADのSAH(2)のKEYH(2)を用いて復号し、SAの継続通知のカプセル化を解き、内部IPパケットを得る。これにより、ユーザFが移動し、端末を変更した場合であっても、SA

が継続される。

【0057】通信相手ホスト3では、ユーザFのSAを継続するために、図4(c)のSPDを検索し、ユーザFに関連するすべての情報を検出する。検出したSPDのなかでユーザFに関するものはSPH(1)とSPH(2)であるため、通信相手ホスト3では、関連するSAH(1)とSAH(2)のSADを調べる。ここでは、SAH(1)のdestinationアドレスがCoA(1)に設定され、端末12の自局IPアドレスと異なっているため、通信相手ホスト3では、端末12の自局IPアドレスをCoA(2)に書き換え、図6(a)に示すSADを図6(b)のように更新する。

【0058】その結果、ユーザFが現在通信している相手、すなわち、通信相手ホスト3は、すべてのセキュリティアソシエーションのdestinationアドレスが“CoA(2)”に変化するため、IPSECトンネルのendpointは、“CoA(1)”から“CoA(2)”に切り替わる。これにより、ユーザFが移動し、端末を変更した場合であっても、セキュリティアソシエーションが維持保証される(図3、ステップS5およびS6、(5)、(6)参照)。

【0059】つぎに、ユーザGが端末11から通信相手ホスト3に対してアクセスする場合について説明する。なお、ユーザGが所有しているICカード内には、図4(b)に示すSPDが保持されている。また、図示はしていないが、端末11は、適切な鍵管理プロトコル：IKEを使用して通信相手ホスト3とのセキュリティアソシエーション：SAを確立する。セキュリティアソシエーション：SAを確立する場合の識別子は、端末11側がユーザGのID(詳細にはX.509のユーザGの認証書のsubject名)であり、通信相手ホスト3が自局IPアドレス：CNまたは通信相手ホスト3の認証書のIDである。

【0060】図7は、ユーザGに関するSADを示す図であり、詳細には、セキュリティアソシエーション：SAを確立後に生成される端末11のセキュリティアソシエーション・データベース：SADの一例を示す図である。なお、使用するIPSECプロトコルはESPを想定する。

【0061】端末11が通信相手ホスト3に対してTCP/UDPのport番号23のパケットを送信する場合、端末11では、図4(b)に示すSPDを検索し、SPG(1)を選択する。SPG(1)には、セキュリティアソシエーションとしてSAG(1)を参照するように記述されているので、図7のSAG(1)を参照する。SAG(1)には、destinationアドレスとして“CN”が、protocolとして“ESP”が、modeとして“tunnel”が指定されているので、端末11では、通信相手ホスト3へのパケットをIPSECでカプセル化し、そのパケットのsou

sourceアドレスを“CoA(1)”とし、destinationアドレスを“CN”とし、SPIを“h(4)”とし、ESPにこれらを付与して送信する。カプセル化の処理では、暗号鍵: KEYH(4)を用いて内側のパケットを暗号化する。

【0062】このパケットを受信した通信相手ホスト3では、(dst, SPI) = (CN, h(2))であるセキュリティアソシエーションを、図6(a)あるいは図6(b)のようなSADから検索する。そして、通信相手ホスト3では、得られたセキュリティアソシエーションを使用してESPを検証し、カプセル化を外して移動端末2からのパケットを得る。カプセル化を外す処理では、暗号鍵: KEYH(4)を用いて内側のパケットを復号する。なお、通信相手ホスト3から端末11へのユーザGに関するパケットも同様に処理される。

【0063】このように、端末11と通信相手ホスト3間のIPSEC通信では、ユーザF、ユーザGともに、端末に設定されているIPアドレスとは独立して通信を行うことができる。

【0064】以上、本実施の形態においては、端末のサブネットワーク間の移動に加えて、ユーザが使用する端末を変更した場合についても対応することとした。すなわち、ICカードに移動前の端末のX.509の認証書を保持し、その内容を移動後の端末に書き込むことによって、セキュリティアソシエーションの再確立に関する処理をなくし、再確立に伴う鍵共有プロトコル: IKEによる「DiffieHellman演算」や「RSA演算」のべき乗剰余演算処理を行わない構成とした。これにより、ユーザが通信に使用する端末を変更した場合であっても、無駄な演算時間を消費することなく、セキュリティアソシエーションを継続することができる。

【0065】なお、図3(4)のSA継続通知では、port番号として10000を使用しているが、10000固定である必要はなく、他の番号でもよい。

【0066】また、本実施の形態では、暗号鍵を用いたIPカプセル化の一例を示したが、IPSECの規格にあるような鍵付きハッシュ関数を用いたデータ認証やデータ圧縮によるIPカプセル化を行った場合であっても、同様の効果を得ることができる。

【0067】また、本実施の形態では、SPDを記録する媒体およびSADを記録する媒体として、ICカードを用いることとしたが、これに限らず、フロッピーディスクや光ディスクなどの別の記録媒体を用いることとしてもよい。また、すべてのSPDとSADを移動後の端末に対して直接入力することとしてもよい。

【0068】また、本実施の形態では、移動前の端末11と通信相手ホスト3との間の通信、および移動後の端末12と通信相手ホスト3との間の通信に、IPSECのトンネルモードを使用した。これに限らず、IPSECのトランスポートモード(Transport Mode)を使用

することとしてもよい。

【0069】また、本実施の形態では、通信相手ホスト3を通信における終端端末として説明したが、これに限らず、ルータなどの中継装置がIPSECのカプセル化による通信を行っている場合でもよい。

【0070】実施の形態2. つぎに、実施の形態2のセキュリティアソシエーション切断/継続方法について説明する。前述の実施形態1では、ユーザFの移動に伴って使用端末を変更した場合に、移動後の端末においてもユーザFに関するセキュリティアソシエーション: SAを継続するようにした。実施の形態2においては、ユーザFが使用する端末を変更した後に、何らかの理由により必要が無くなったセキュリティアソシエーション: SAを切断する。なお、通信システムのネットワーク構成については、前述の実施の形態1と同様のため同一の符号を付してその説明を省略する。

【0071】図8は、実施の形態2のセキュリティアソシエーション切断/継続方法を示す図であり、詳細には、通信相手ホスト3と端末11との間および通信相手ホスト3と端末12との間において、セキュリティアソシエーションを切断するシーケンスを示す図である。

【0072】ここで、実施の形態2のセキュリティアソシエーション切断/継続方法について説明する。なお、図8(1), (2), (3)の処理については、前述の実施の形態1と同様である。

【0073】ユーザFは、使用する端末を端末11から端末12へ変更する場合、ICカード14に記録された図5(a)に示すSADを、端末12へ書き込む。端末12では、図5(a)の受信用SAF(2)のdestinationアドレスが端末12の自局アドレスと異なるため、CoA(1)を端末12のIPアドレスであるCoA(2)へ変更する。これにより、図5(a)のセキュリティ・アソシエーション・データベース: SADの内容は図5(b)のように更新される。

【0074】さらに、端末12では、通信相手ホスト3に対して、ユーザFに関するセキュリティ・アソシエーション・データベース: SADに従ってセキュリティアソシエーション: SAを切断する旨を通知する(図8, ステップS11, (4)参照)。ここでは、sourceアドレスを“CoA2”とし、destinationアドレスを“CN”とし、SPIを“h(2)”とし、ESPにこれらを付与する。そして、内側のパケットのsourceアドレスを“CoA(2)”とし、destinationアドレスを“CN”とし、port番号を“10000”とし、データ部にSAを切断するコードとユーザFの認証書のsubject名を設定し、暗号鍵: KEYH(2)を用いて暗号化し、IPSECでカプセル化を行う。

【0075】SA切断通知を受信した通信相手ホスト3では、(dst, SPI) = (CN, h(2))である

セキュリティアソシエーションを、図6(a)のSADから検索する。そして、内側のパケットを、SADのSAH(2)のKEYH(2)を用いて復号し、さらに、SA継続通知のIPSECによるカプセル化を解き、内部IPパケットを得る。その後、通信相手ホスト3では、ユーザFのSAを切断する処理を行う。

【0076】通信相手ホスト3では、ユーザFのSAを切断するために、図4(c)のSPDを検索し、ユーザFに関連するすべての情報を検出する。検出したSPDでユーザFに関する情報はSPH(1)とSPH(2)であるので、保持している図6のSAH(1)とSAH(2)を消去し、セキュリティアソシエーション:SAを開放する。その後、通信相手ホスト3と端末12との間に、新たなセキュリティアソシエーションを再確立する。

【0077】このように、本実施の形態においては、通信に使用する端末の変更に伴って不要になったセキュリティアソシエーションを、寿命が終了する前に切断することとした。これにより、無駄なリソースの消費を抑制することができる。

【0078】なお、図8(4)のSA切断通知では、port番号として“10000”を使用しているが、10000固定である必要はなく、他の番号でもよい。

【0079】また、本実施の形態では、暗号鍵を用いたIPカプセル化の一例を示したが、これに限らず、IPSECの規格にあるような鍵付きハッシュ関数を用いたデータ認証やデータ圧縮によるIPカプセル化を行った場合であっても、同様の効果を得ることができる。

【0080】また、本実施の形態では、SPDを記録する媒体およびSADを記録する媒体として、ICカードを用いることとしたが、これに限らず、フロッピーディスクや光ディスクなどの別の記録媒体を用いることとしてもよい。また、すべてのSPDとSADを移動後の端末に対して直接入力することとしてもよい。

【0081】また、本実施の形態では、移動前の端末11と通信相手ホスト3との間の通信、および移動後の端末12と通信相手ホスト3との間の通信に、IPSECのトンネルモードを使用した。これに限らず、IPSECのトランスポートモード(Transport Mode)を使用することとしてもよい。

【0082】また、本実施の形態では、通信相手ホスト3を通信における終端端末として説明したが、これに限らず、ルータなどの中継装置がIPSECのカプセル化による通信を行っている場合でもよい。

【0083】

【発明の効果】以上、説明したとおり、本発明によれば、ユーザが使用する端末を変更した場合についても対応することとした。具体的にいうと、ICカードに第1の端末のX.509の認証書を保持し、その内容を第3の端末に書き込むことによって、セキュリティアソシエ

ーションの再確立に関する処理をなくし、再確立に伴う鍵共有プロトコル:IKEによる「DiffieHellman演算」や「RSA演算」のべき乗剰余演算処理を行わないこととした。これにより、ユーザが通信に使用する端末を変更した場合であっても、無駄な演算時間を消費することなく、既に確立されているセキュリティアソシエーションを継続することができる、という効果を奏する。

【0084】つぎの発明によれば、通信に使用する端末の変更に伴って不要になったセキュリティアソシエーションを、寿命が終了する前に切断することとした。これにより、無駄なリソースの消費を抑制することができる、という効果を奏する。

【0085】つぎの発明によれば、ICカードに第1の端末のX.509の認証書を保持し、その内容を第3の端末に書き込むことによって、セキュリティアソシエーションの再確立に関する処理をなくし、再確立に伴う鍵共有プロトコル:IKEによる「DiffieHellman演算」や「RSA演算」のべき乗剰余演算処理を行わない構成とした。これにより、ユーザが通信に使用する端末を変更した場合であっても、無駄な演算時間を消費することなく、既に確立されているセキュリティアソシエーションを継続することが可能な通信システムを得ることができる、という効果を奏する。

【0086】つぎの発明によれば、通信に使用する端末の変更に伴って不要になったセキュリティアソシエーションを、寿命が終了する前に切断することとした。これにより、無駄なリソースの消費を抑制することが可能な通信システムを得ることができる、という効果を奏する。

【図面の簡単な説明】

【図1】 本発明にかかるセキュリティアソシエーション切断/継続方法を実現する通信システムの構成を示す図である。

【図2】 IPSECを用いた端末間の通信の様子を示す図である。

【図3】 ユーザFが端末11から端末12へ移動した場合の動作シーケンスの一例を示す図である。

【図4】 ユーザFの持つICカード内のSPD、ユーザGの持つICカード内のSPD、通信相手ホスト3内のSPD、を示す図である。

【図5】 ユーザFに関するSADを示す図である。

【図6】 通信相手ホスト3に関するSADを示す図である。

【図7】 ユーザGに関するSADを示す図である。

【図8】 実施の形態2のセキュリティアソシエーション切断/継続方法を示す図である。

【図9】 従来のセキュリティアソシエーション切断/継続方法を示す図である。

【図10】 移動端末102から通信相手ホスト103

へIPSECトンネルを用いてパケットを転送する様子
を示す図である。

【図11】 移動端末102および通信相手ホスト103
が接続されたネットワークの動作手順を示す図であ
る。

【図12】 サブネットワーク101aに存在する移動
端末102が通信相手ホスト103と通信を行う場合の
動作シーケンスの一例を示す図である。

【図13】 移動端末102および通信相手ホスト10

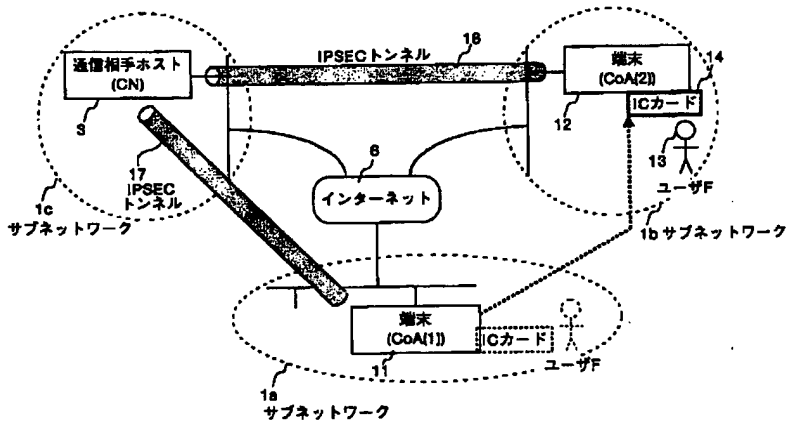
3が持つSPDの一例を示す図である。

【図14】 移動端末102および通信相手ホスト10
3が持つSADの一例を示す図である。

【符号の説明】

1a, 1b, 1c サブネットワーク、3 通信相手ホ
スト(CN)、6 インターネット、11, 12 端
末、13 ユーザF、14 ICカード、17, 18
IPSECトンネル、102 移動端末、103 通信
相手ホスト、107, 108 IPSECトンネル。

【図1】

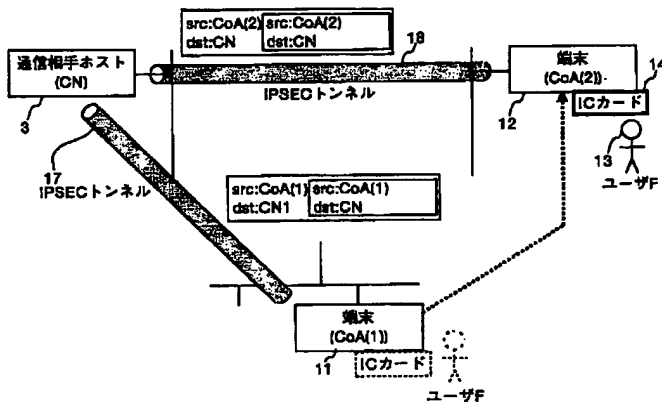


【図7】

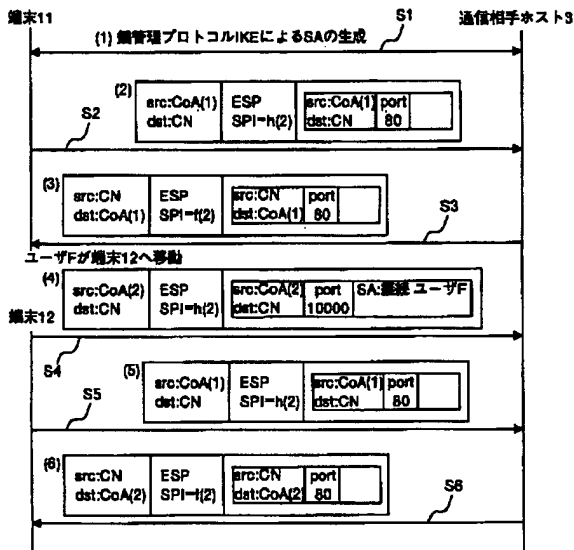
端末11内のユーザGに関するSAD

識別名	field	値
SAG(1) (送信用)	dst	CN
	proto	ESP
	mode	tunnel
	SPI	h(4)
	暗号鍵 その他情報	KEYH(4) *****
SAG(2) (受信用)	dst	CoA(1)
	proto	ESP
	mode	tunnel
	SPI	g(2)
	暗号鍵 その他情報	KEYG(2) *****

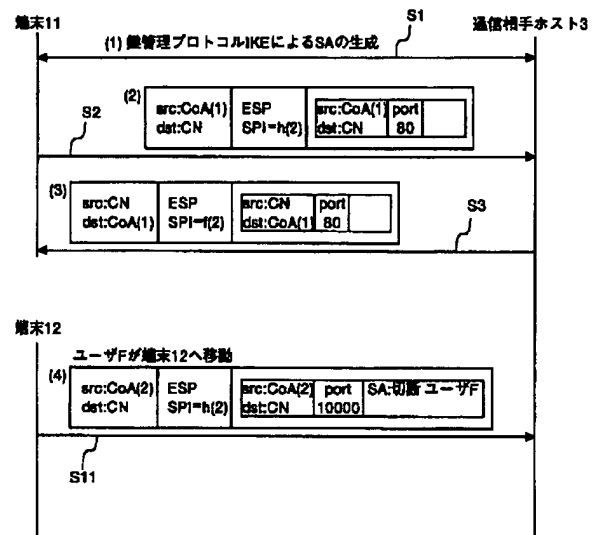
【図2】



【図3】



【図8】



【図4】

(a) ユーザFのICカード内のSPD

識別名	field	値
SPF(1)	src	any(don't care)
	dst	CN
	ユーザID	ユーザF
	port	80,10000
(送信用)	SA	SAF(1)
SPF(2)	src	CN
	dst	any(don't care)
	ユーザID	ユーザF
	port	80,10000
(受信用)	SA	SAF(2)

(b) ユーザGのICカード内のSPD

識別名	field	値
SPG(1)	src	any(don't care)
	dst	CN
	ユーザID	ユーザG
	port	23,10000
(送信用)	SA	SAG(1)
SPG(2)	src	CN
	dst	any(don't care)
	ユーザID	ユーザG
	port	23,10000
(受信用)	SA	SAG(2)

(c) 通信相手ホスト3内のSPD

識別名	field	値
SPH(1)	src	CN
	dst	any(don't care)
	ユーザID	ユーザF
	port	80,10000
(送信用)	SA	SAH(1)
SPH(2)	src	any(don't care)
	dst	CN
	ユーザID	ユーザF
	port	80,10000
(受信用)	SA	SAH(2)
SPH(3)	src	CN
	dst	any(don't care)
	ユーザID	ユーザG
	port	23,10000
(送信用)	SA	SAH(3)
SPH(4)	src	any(don't care)
	dst	CN
	ユーザID	ユーザG
	port	23,10000
(受信用)	SA	SAH(4)

【図13】

(a) 移動端末102内のSPD

識別名	field	値
SPM(1)	src	Haddr
	dst	CN
	ユーザID	ユーザF
	port	80,10000
(送信用)	SA	SAM(1)
SPM(2)	src	CN
	dst	Haddr
	ユーザID	ユーザG
	port	23,10000
(受信用)	SA	SAM(2)

(b) 通信相手ホスト103内のSPD

識別名	field	値
SPC(1)	src	CN
	dst	Haddr
	ユーザID	ユーザF
	port	80,10000
(送信用)	SA	SAC(1)
SPC(2)	src	Haddr
	dst	CN
	ユーザID	ユーザG
	port	23,10000
(受信用)	SA	SAC(2)

【図5】

(a)
端末11からユーザFのICカードへコピーするSAD

識別名	field	値
SAF(1) (送信用)	dst	CN
	proto	ESP
	mode	tunnel
	SPi	h(2)
	暗号鍵 その他情報	KEYH(2) *****
SAF(2) (受信用)	dst	CoA(1)
	proto	ESP
	mode	tunnel
	SPi	f(2)
	暗号鍵 その他情報	KEYF(2) *****

(b)
ユーザFのICカードから端末12へコピー後のSAD

識別名	field	値
SAF(1) (送信用)	dst	CN
	proto	ESP
	mode	tunnel
	SPi	h(2)
	暗号鍵 その他情報	KEYH(2) *****
SAF(2) (受信用)	dst	CoA(2)
	proto	ESP
	mode	tunnel
	SPi	f(2)
	暗号鍵 その他情報	KEYF(2) *****

【図6】

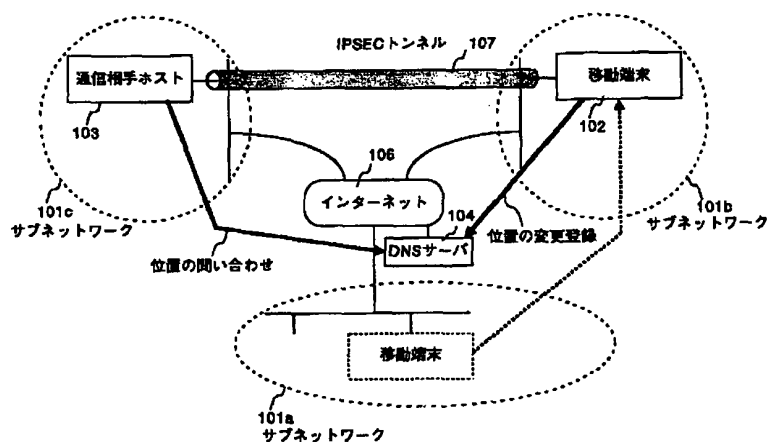
(a)
通信相手ホスト3内のSAD(変更前)

識別名	field	値
SAH(1) (送信用)	dst	CoA(1)
	proto	ESP
	mode	tunnel
	SPi	f(2)
	暗号鍵 その他情報	KEYF(2) *****
SAH(2) (受信用)	dst	CN
	proto	ESP
	mode	tunnel
	SPi	h(2)
	暗号鍵 その他情報	KEYH(2) *****
SAH(3) (送信用)	dst	CoA(1)
	proto	ESP
	mode	tunnel
	SPi	g(2)
	暗号鍵 その他情報	KEYG(2) *****
SAH(4) (受信用)	dst	CN
	proto	ESP
	mode	tunnel
	SPi	h(4)
	暗号鍵 その他情報	KEYH(4) *****

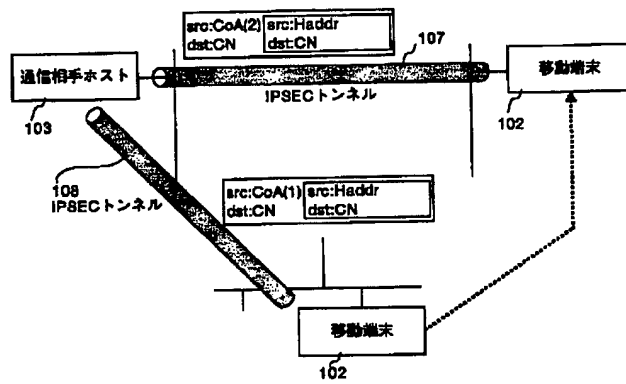
(b)
通信相手ホスト3内のSAD(変更後)

識別名	field	値
SAH(1) (送信用)	dst	CoA(2)
	proto	ESP
	mode	tunnel
	SPi	f(2)
	暗号鍵 その他情報	KEYF(2) *****
SAH(2) (受信用)	dst	CN
	proto	ESP
	mode	tunnel
	SPi	h(2)
	暗号鍵 その他情報	KEYH(2) *****
SAH(3) (送信用)	dst	CoA(1)
	proto	ESP
	mode	tunnel
	SPi	g(2)
	暗号鍵 その他情報	KEYG(2) *****
SAH(4) (受信用)	dst	CN
	proto	ESP
	mode	tunnel
	SPi	h(4)
	暗号鍵 その他情報	KEYH(4) *****

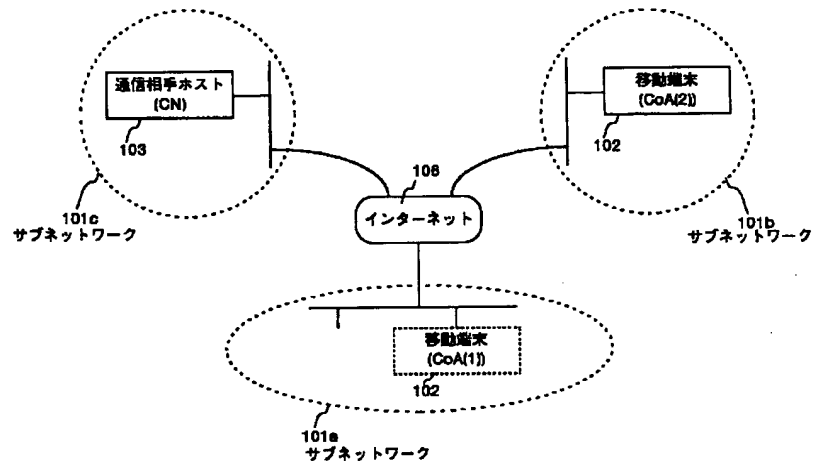
【図9】



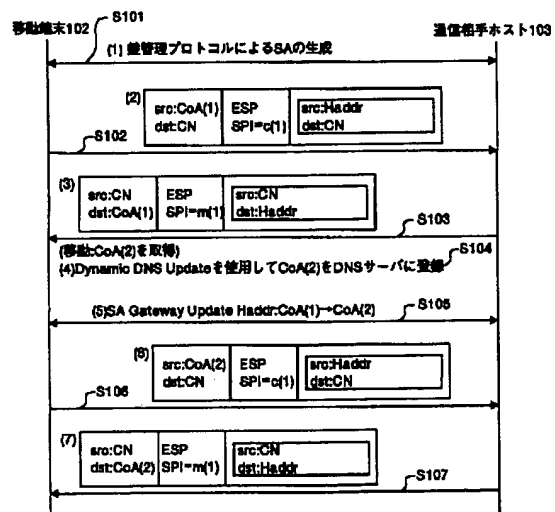
【図10】



【図11】



【図12】



【図14】

(a) 移動端末102内のSAD(変更前)			(b) 通信相手ホスト103内のSAD(変更前)		
識別名	field	値	識別名	field	値
SAM(1) (送信用)	dst	CN	SAC(1) (送信用)	dst	CoA(1)
	proto	ESP		proto	ESP
	mode	tunnel		mode	tunnel
	SPI	c(1)		SPI	m(1)
	その他情報	*****		その他情報	*****
SAM(2) (受信用)	dst	CoA(1)	SAC(2) (受信用)	dst	CN
	proto	ESP		proto	ESP
	mode	tunnel		mode	tunnel
	SPI	m(1)		SPI	c(1)
	その他情報	*****		その他情報	*****
(c) 移動端末102内のSAD(変更後)			(d) 通信相手ホスト103内のSAD(変更後)		
識別名	field	値	識別名	field	値
SAM(1) (送信用)	dst	CN	SAC(1) (送信用)	dst	CoA(2)
	proto	ESP		proto	ESP
	mode	tunnel		mode	tunnel
	SPI	c(1)		SPI	m(1)
	その他情報	*****		その他情報	*****
SAM(2) (受信用)	dst	CoA(2)	SAC(2) (受信用)	dst	CN
	proto	ESP		proto	ESP
	mode	tunnel		mode	tunnel
	SPI	m(1)		SPI	c(1)
	その他情報	*****		その他情報	*****

 フロントページの続き

(72)発明者 後沢 忍
 東京都千代田区丸の内二丁目2番3号 三
 菱電機株式会社内

Fターム(参考) 5B085 AA03 AE02 AE15 AE23 AE29
 BC02 BG07 CC03
 5B089 GB01 KA12 KA17 KB06
 5J104 AA01 AA16 EA02 EA04 EA26
 NA02 NA35 PA07
 5K030 GA01 GA15 JT09 LD19